TECHNIQUES FOR COMPOSITIONAL AND SYMBOLIC ANALYSIS OF SOFTWARE PRESENTED AT SPIN'06

HIGHLIGHT: Two papers describing work by the Robust Software Engineering Group on compositional and symbolic reasoning for software verification were presented at the 13th International SPIN Workshop on Model Checking of Software, part of ETAPS (The European Joint Conferences on Theory and Practice of Software). The conference was held in Vienna, Austria March 30-April 1, 2006.

- "Towards a Compositional SPIN" by Corina S. Pasareanu and Dimitra Giannakopoulou (QSS and RIACS/NASA Ames Research Center) describes automated compositional verification applied to a design model of the MER arbiter (a flight software module from JPL's Mars Exploration Rovers) in the context of the SPIN verification tool. Compositional verification achieved 100x savings in memory, as compared to traditional (non-compositional) verification.

- "Symbolic Execution with Abstract Subsumption Checking" by Saswat Anand (Georgia Institute of Technology), Corina S. Pasareanu (QSS/NASA Ames Research Center), and Willem Visser (RIACS/NASA Ames Research Center) describes novel approximate algorithms for performing state comparison during symbolic analysis of code. These algorithms enable pruning large portions of the explored program state space, therefore enabling more efficient verification.

BACKGROUND: The goal of the Reliable Software/Flight Control Algorithms project is to improve the reliability and safety of software systems to support human and robotic exploration of space. The project will provide an integrated environment for the development of software and its verification and validation, throughout the life cycle. For the past few years, we have worked on developing tools for the automated verification of software designs and code. In order to apply these tools to large NASA projects, it is imperative to scale up the size of systems that can be mathematically analyzed.

Two key techniques in achieving scalability in the verification of large software systems are compositional and symbolic reasoning. Compositional reasoning is a "divide and conquer" technique that breaks up the verification of a system into smaller tasks that involve the verification of its components, while symbolic reasoning represents program data with symbolic values and constraints to enable automated analysis of multiple (possibly an infinite number of) program executions all at once.

PROGRAM FUNDING: Exploration Systems Mission Directorate, Explorations Systems Research & Technology Program 6G: Reliable Software/Flight Control Algorithms

POC: Corina Pasareanu, pcorina@email.arc.nasa.gov